Full Speed Ahead: NMCI Underway on Digital Power

By Eric T. Mazzacone,
PEO-IT Public Affairs

ARLINGTON, Va. — The Navy-designated approval authority granted interim authority to operate to the Norfolk and San Diego Network Operations Centers and Help Desks Aug. 13. Following this decision, the Defense Information Systems Agency Security Accreditation Group granted these facilities an interim authority to connect to the unclassified but sensitive Internet protocol router network known as the NIPRNet August 16.

The interim authority to operate grants the NMCI team the ability to operate, certifying that it can do so within "a manageable level of security risks," according to Scott Henderson, NMCI Information Assurance division head with Space and Naval Warfare Systems Command in San Diego. With this milestone reached the obstacle to be tackled was the attainment of the interim authority to connect.

"The interim authority to operate is an internal certification. It's someone within your program stating that you have satisfied your testing and reporting requirements and your network is therefore ready to begin operation," Henderson said.

In order to attain the interim authority to operate, the NMCI program manager had to prove to the designated approval authority that they were operating within an acceptable level of manageable risk in accordance with Department of Defense and Department of the Navy policy. Among other methods used by the program manager to test the network's security, security assessment teams were used to attempt network infiltration. Having successfully passed these tests, the network was ready to reach for its next critical approval, the interim authority to connect.

To attain this goal, the program manager and NMCI designated approval authority had to provide the Defense Information Systems Network designated approval authority with a full security testing report, risk assessment analysis and a system security authorization agreement.

"We had to prove that NMCI was operating compatibly within NIPRNet security parameters, and Defense Department certification and accreditation policy," said Henderson.

The Defense Information Systems Network designated approval authority granted the Network Operations Centers and Help Desks the interim authority to connect until September 30. During this time, SPAWAR's Program Management Office must complete further security testing and reporting in order to be granted an extension.

"Obtaining the interim authority to connect is perhaps one of the most important things to happen within the scope of the NMCI contract so far. This authority enables the NMCI to connect directly to the NIPRNet," stated Henderson. "It is this connectivity that allows the Department of the Navy to conduct testing of NMCI over the NIPRNet, which is the first step in the cut-over of seats to the network."

Since the NIPRNet is the unclassified but sensitive wide-area network used by the entire Defense Department, connecting to it allows NMCI to communicate with Joint users.

"Things are going well with the testing and reporting requirements to maintain our connectivity," explained Henderson. "We are working to complete action items requested by the NMCI designated approval authority. And, we are currently working toward obtaining an extended authority to operate. With that extension, we will begin to roll out additional NIPRNet sites connected to the NMCI. We'll also be pursuing our approval to connect the NMCI to the Secret Internet Protocol Router Network or SIPRNet."

For more information on the Navy Marine Corps Intranet, go to http://www.spawar.navy.mil